# Asirによる有限群の不変式環の生成元の計算 (Computer Algebra : Algorithms, Implementations and Applications)

AUTHOR(S):

渡邊, 芳英; 鍋島, 勇

数理解析研究所講究録 1295 巻 2002 年 17-28



# Asir による有限群の不変式環の生成元の計算

同志社大学工学部　渡邊 芳英　(Yoshihide WATANABE) *
NEC　鍋島 勇　(Isamu NABESHIMA)

## 1 はじめに

本稿の目的は標数0の体に係数をもつ有限行列群の不変式環の生成元を計算するアルゴリズムを数式処理システム Asir に実装することである. ここで用いるアルゴリズムは本質的には B.Sturmfels によるもの ([13]) であるが, 詳細については, E.H.Agnes による Singular への実装の ドキュメント ([1]) を参考にして, 些細な変更, 改良を行った. ここではその概要を述べるが, 詳細については [9] を参照されたい. 他のアルゴリズムとして, 係数体の標数が任意の場合にでも適用できる G.Kemper のアルゴリズム ([7]) が知られているが, ここでは様々な理由で取り上げることが出来なかった.

## 2 有限行列群の不変式環の構造

### 2.1 次数付多元環としての不変式環

$\mathbb{F}$ を標数0の体として, 自然数 $n$ に対して, $n$ 個の変数 $x_1, x_2, \ldots, x_n$ に関する $\mathbb{F}$ 係数多項式環を $\mathbb{F}[x_1, \ldots, x_n]$ で表わす. 一般線形群 $\mathrm{GL}(\mathbb{F}^n)$ の有限部分群 $\Gamma \subset \mathrm{GL}(\mathbb{F}^n)$ に対して, $\Gamma$ の $\mathbb{F}[x_1, \ldots, x_n]$ への作用 (表現) を任意の $\pi = (\pi_{ij})_{1 \leq i,j \leq n} \in \Gamma$ に対して

$$\begin{array}{rccl} \omega_\pi : & \mathbb{F}[x_1, \ldots, x_n] & \to & \mathbb{F}[x_1, \ldots, x_n] \\ & f(x_1, \ldots, x_n) & \mapsto & f(\sum_{j=1}^{n} \pi_{1j} x_j, \ldots, \sum_{j=1}^{n} \pi_{nj} x_j) \end{array} \tag{1}$$

で定義する. 変数 $x_1, \ldots, x_n$ からなる列ベクトルを $\mathbf{x}$ で表わせば, (1) は簡単に,

$$\omega_\pi(f(\mathbf{x})) = f(\pi \cdot \mathbf{x})$$

となる.

**定義 2.1** 多項式 $f \in \mathbb{F}[x_1, \ldots, x_n]$ は, 作用 $\omega_\pi$ ($\pi \in \Gamma$) で不変であるとき, すなわち

$$f(\mathbf{x}) = f(\pi \cdot \mathbf{x}) \qquad \forall \pi \in \Gamma$$

であるとき, $\Gamma$ で不変であると呼ばれる. また, $\Gamma$ で不変な多項式 (不変式) 全体を $\mathbb{F}[x_1, \ldots, x_n]^\Gamma$ で表わす. $\mathbb{F}[x_1, \ldots, x_n]^\Gamma$ は $\mathbb{F}[x_1, \ldots, x_n]$ の, 単位元を持つ部分環であり, さらに $\mathbb{F}$ を含む $\mathbb{F}$ 上の多元環である. これを $\Gamma$ の**不変式環**と言う.

*Email:yoshi@gandalf.doshisha.ac.jp

多項式 $f \in \mathbb{F}[x_1,\ldots,x_n]$ が $\Gamma$ に関して不変であることと, $f$ のすべての同次部分が $\Gamma$ で不変であることは同値である. 特に, 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ は $\mathbb{F}$ 上の次数付多元環であり, $\mathbb{F}[x_1,\ldots,x_n]^\Gamma_d$ を次数 $d \in \mathbb{N}_0$ の同次不変式全体で生成される

## 2.2 Reynolds 作用素と Noether の定理

**定義 2.2** 以下で定義される作用素 $R_\Gamma$ を有限行列群 $\Gamma$ の **Reynolds 作用素**という.

$$\begin{aligned} R_\Gamma : \mathbb{F}[x_1,\ldots,x_n] &\to \mathbb{F}[x_1,\ldots,x_n] \\ f &\mapsto \frac{1}{|\Gamma|}\sum_{\pi\in\Gamma} f(\pi\cdot\mathbf{x}) = \frac{1}{|\Gamma|}\sum_{\pi\in\Gamma}\omega_\pi(f) \end{aligned}$$

**命題 2.3**

(1) $f \in \mathbb{F}[x_1,\ldots,x_n]$ なら, $R_\Gamma(f) \in \mathbb{F}[x_1,\ldots,x_n]^\Gamma$ であり, また任意の $d \in \mathbb{N}_0$ について, $R_\Gamma(\mathbb{F}[x_1,\ldots,x_n]_d) = \mathbb{F}[x_1,\ldots,x_n]^\Gamma_d$ である.

(2) Reynolds 作用素 $R_\Gamma$ は $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ 上では恒等写像になる.

**系 2.4** $\mathbb{F}[x_1,\ldots,x_n]^\Gamma_d$ は $\mathbb{F}[x_1,\ldots,x_n]_d$ の単項式 $m$ に Reynolds 作用素を作用させたもの $R_\Gamma(m)$ 全体で生成される. また $R_\Gamma(m)$ のうち 1 次独立なものを $R_\Gamma(m_1),\ldots,R_\Gamma(m_k)$ とすれば, これら $k$ 個の同次式が $\mathbb{F}[x_1,\ldots,x_n]^\Gamma_d$ を生成して $\dim_\mathbb{F}(\mathbb{F}[x_1,\ldots,x_n]^\Gamma_d) = k$ である.

さらにこのような Reynolds 作用素により, 不変式環のすべての生成元が作られて, 不変式環は $\mathbb{F}$ 上の有限生成の多元環となる.

**定理 2.5** (**Noether** 1916[10]) 有限群 $\Gamma \subset \mathrm{GL}(\mathbb{F}^n)$ の位数を $|\Gamma|$ とする. そのとき, 全次数が $|\Gamma|$ 以下の単項式,

$$\mathbf{x}^\beta = x_1^{\beta_1}\cdots x_n^{\beta_n} \quad (|\beta| = \beta_1 + \cdots + \beta_n \le |\Gamma|)$$

に対して Reynolds 作用素を作用させて得られた不変式の全体を $S$ で表わせば, 群 $\Gamma$ の任意の不変式を $S$ の元の多項式で表わすことが出来る.

## 2.3 Hilbert 級数と Molien の定理

**定義 2.6** 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ は $\mathbb{F}$ 上の次数付多元環であり, 空間 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma_d$ は $\mathbb{F}[x_1,\ldots,x_n]_d$ の部分空間なので有限次元になるから $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の **Hilbert 級数** $H_\Gamma(X)$ を

$$H_\Gamma(X) := \sum_{d\in\mathbb{N}_0} \dim_\mathbb{F}(\mathbb{F}[x_1,\ldots,x_n]^\Gamma_d)X^d$$

で定義することができる.

次の古典的な定理は不変式環の Hilbert 級数を与える.

**定理 2.7** (**Molien**,1897,[8])
不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の Hilbert 級数 $H_\Gamma(X)$ は,

$$\frac{1}{|\Gamma|}\sum_{\pi\in\Gamma}\frac{1}{\det(I-X\cdot\pi)}$$

で与えられる. 但し, $I$ は $n$ 次の単位行列である.

この定理により, 同次不変式のなすベクトル空間の次元が計算でき, またその同次不変式のなすベクトル空間の基底は Reynolds 作用素を用いて生成することができる. さらに, Noether の定理により, 不変式環全体は有限生成であって, 生成元の次数の上限がわかっているから, このような Reynolds 作用を用いた生成元の生成の操作は有限回で終了し, 冗長さを許すなら, 不変式環の生成元をすべて求めることができる.

しかし, このような方法で不変式環の生成元を求めることが出来たとしても, その中には冗長な生成元が含まれている可能性がある. その場合, ある生成元が他の生成元の多項式として表わされることになる. また, 生成元の間に代数的な関係式がある可能性もある. 前者の場合, そのような無駄な生成元は取り除くべきだろう. 後者の場合はそのような代数的な関係式がどのようなものであるか見いだす必要がある. 次の節では不変式環の構造をもう少し立ち入って記述する.

## 2.4 不変式環の超越次数

**定義 2.8** $S$ は環で $R$ を部分環として含むとする. 要素 $a\in S$ が $R$ 上で**整元**であると言われるのは, $a$ が, $R$ の要素を係数に持つ最高次の係数が 1 の多項式の根になっている時である. また, $S$ のすべての要素が $R$ 上で整元であれば, 環 $S$ は $R$ 上で**整である**と呼ばれる.

次の命題 2.9 の証明は容易であるが基本的である ([13]).

**命題 2.9** 多項式環 $\mathbb{F}[x_1,\ldots,x_n]$ は $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ 上で整である.

**定義 2.10** (**代数拡大と超越拡大**) 体 $K$ の拡大体を $L$ とする.

(1) 拡大 $L\supseteq K$ は環の拡大 $L\supseteq K$ が整であるとき, $K$ の**代数拡大**であるという. $L\supseteq K$ が代数拡大でないとき**超越的拡大**という.

(2) 拡大 $L\supseteq K$ において $B\subset L$ が, $K$ 上で代数的に独立な最大の集合であるとき, $B$ を超越拡大 $L\supseteq K$ の**超越基底**という.

(3) 体の拡大 $L\supseteq K$ が有限個の超越基底をもつとき, その超越基底の数は超越基底の選び方によらない. この数を $L\supseteq K$ の**超越次数**といい, $\mathrm{trdeg}_K(L)$ で表わす.

(4) $R$ を整域, $K$ を体として, $R\supseteq K$ を環の拡大とする. そのとき整域 $R$ の体 $K$ 上の超越次数を商体 $Q(R)$ の $K$ 上の超越次数で定義し, これを $\mathrm{trdeg}_K(R)$ と表わす.

命題 2.9 の結果を踏まえて, 直感的には明らかな命題

**命題 2.11** $S \supseteq R$を整域の拡大で, $S$は$R$上整であるとし, $R$は体$\mathbb{F}$を含み, $\mathrm{trdeg}_{\mathbb{F}}(S) = n$とする. このとき, $\mathrm{trdeg}_{\mathbb{F}}(R) = n$となる. すなわち, $R$の部分集合の中で$\mathbb{F}$上で代数的に独立な要素の個数は最大$n$個となる.

を，整域の拡大（代数拡大）$S = \mathbb{F}[x_1, \ldots, x_n] \supset \mathbb{F}[x_1, \ldots, x_n]^\Gamma = R$に当てはめれば，次の定理が得られる.

**定理 2.12** 有限行列群$\Gamma$の不変式環$\mathbb{F}[x_1, \ldots, x_n]^\Gamma$の$\mathbb{F}$上の超越次数は$n$である. すなわち, $\mathbb{F}[x_1, \ldots, x_n]^\Gamma$の部分集合の中で$\mathbb{F}$上で代数的に独立な要素の最大個数は$n$である.

この定理から不変式環の代数的に独立な生成元の個数は$n$であることがわかる.

## 2.5 Noetherの正規化定理と Cohen-Macaulay 環

前節で不変式環の生成元のうちで代数的に独立なものの数は丁度変数の数$n$に等しいことが分かった. 本節では不変式環の構造をさらに詳しく述べる.

**定理 2.13 Noetherの正規化定理**
$A \neq \{0\}$を有限生成な$\mathbb{F}$上の次数付多元環として, $A$の$\mathbb{F}$上の超越次数を$n$とすると, 次の条件を満たす有限個の同次元$p_1, \ldots, p_n \in A$が存在する.

(1) $p_1, \ldots, p_n$は$\mathbb{F}$上で代数的に独立である.

(2) $A$は$\mathbb{F}[p_1, \ldots, p_n]$上で整である. または同値な言い換えをすれば, $A$は$\mathbb{F}[p_1, \ldots, p_n]$の加群として有限生成である.

**定義 2.14 (Noetherの正規化, パラメータ系)** Noetherの正規化定理2.13中の多元環$\mathbb{F}[p_1, \ldots, p_n]$を, $A$の**Noetherの正規化**と呼ぶ. 今の場合$p_1, \ldots, p_n$はすべて同次式であるから特に同次なNoetherの正規化と呼ぶこともある. また$p_1, \ldots, p_n$を$A$の**同次パラメータ系**と呼ぶ. 同次なパラメータ系はh.s.o.p. (homogeneous system of parameters) と略記されることもある.

$A = \bigoplus_{d \in \mathbb{N}_0} A_d$, $(A_0 = \mathbb{F})$を有限生成な$\mathbb{F}$上の次数付多元環で$A$の$\mathbb{F}$上の超越次数を$n$とすれば, Noetherの正規化定理により代数的に独立な同次元$p_1, \ldots, p_n$が存在し, $A$は多元環$\mathbb{F}[p_1, \ldots, p_n]$上整となる. 同値な言い換えをするなら, $A$は多元環$\mathbb{F}[p_1, \ldots, p_n]$上の有限生成の加群となる. この加群が自由加群となるようなパラメータ系$p_1, \ldots, p_n$が存在するとき, 多元環$A$は**Cohen-Macaulay環**であると呼ばれる. すなわち, 同次なパラメータ系$p_1, \ldots, p_n$を持つ$\mathbb{F}$上の次数付多元環$A$がCohen-Macaulay環であれば, $s_1, \ldots, s_t \in A$が存在して，直和分解

$$A = \bigoplus_{j=1}^{t} s_j \mathbb{F}[p_1, \ldots, p_n] \tag{2}$$

得られる. そのとき

**定義 2.15** 次数付Cohen-Macaulay環$A$の自由加群としての直和分解 (2) を**広中分解**という. さらに$s_1, \ldots, s_t$も同次な場合は**同次な広中分解**という.

次の定理は, 有限行列群の不変式環の一般的な構造について, ほぼ最終的な結果を与える.

**定理 2.16 (Hochster and Eagon [6])**
不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ は Cohen-Macaulay 環であり, 自由加群としての $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の基底は, 同次不変式で構成することができる. 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の同次なパラメータ系を $p_1,\ldots,p_n$ とすれば, 同次な不変式 $s_1,\ldots,s_t \in \mathbb{F}[x_1,\ldots,x_n]^\Gamma$ が存在して, 広中分解 (直和分解)

$$\mathbb{F}[x_1,\ldots,x_n]^\Gamma = \bigoplus_{j=1}^{t} s_j \mathbb{F}[p_1,\ldots,p_n]$$

が得られる. $p_1,\ldots,p_n$ を **Primary Invariants**, $s_1,\ldots,s_t$ を **Secondary Invariants** と呼ぶ.

# 3 不変式環の生成アルゴリズム

## 3.1 Primary Invariants の生成

不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の Primary Invariants を生成する問題は $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の同次なパラメータ系を見いだすことであり, そのためには $n$ 個の代数的に独立な不変式 $p_1,\ldots,p_n$ であって, 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ が多元環 $\mathbb{F}[p_1,\ldots,p_n]$ 上整となるものを見いだせばよい. このような不変式を生成するには Reynolds 作用素を用いればよいが, その際の問題点は次のようなものである.

- Reynolds 作用素により順に生成された不変式の最初の $n$ 個が代数的に独立である可能性は殆んどない. 従って, 代数的に独立でない不変式をどのように取り除いて, 代数的に独立な $n$ 個の不変式を見いだすか.
- もし $n$ 個の代数的に独立な多項式 $p_1,\ldots,p_n$ を見い出したとしても, $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ が $\mathbb{F}[p_1,\ldots,p_n]$ 上で整であるとは限らず, その場合は $p_1,\ldots,p_n$ はパラメータ系にならない.

我々は, 以下で Primary Invariants $p_1,\ldots,p_n$ を見つけるアルゴリズムを提示する. その本質的な部分は,『$p_1,\ldots,p_n$ が不変式環のパラメータ系になる条件, すなわち, 不変式環が $\mathbb{F}[p_1,\ldots,p_n]$ 上整となるための条件』である.

**命題 3.1** ([1]) $p_1,\ldots,p_m \in \mathbb{F}[x_1,\ldots,x_n]^\Gamma$ を次数が正の同次式とする.

(1) 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ が $\mathbb{F}[p_1,\ldots,p_m]$ 上整であるための必要十分条件は,

$$\sqrt{\langle p_1,\ldots,p_m\rangle} = \langle x_1,\ldots,x_n\rangle. \tag{3}$$

である. ここでイデアル $\langle p_1,\ldots,p_m\rangle$ は多項式環 $\mathbb{F}[x_1,\ldots,x_n]$ のイデアルであり, 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の中のイデアルを考えているわけではない. また $\sqrt{\langle p_1,\ldots,p_m\rangle}$ はイデアル $\langle p_1,\ldots,p_m\rangle$ の根基イデアルを表わす.

(2) (1) の条件が満たされるとき, $m \geq n$ が成り立つ. 特に $m = n$ のとき, 部分環 $\mathbb{F}[p_1,\ldots,p_n]$ が $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の Noether の正規化であるための必要十分条件は

$$\sqrt{\langle p_1,\ldots,p_n\rangle} = \langle x_1,\ldots,x_n\rangle \tag{4}$$

である.

上の命題 3.1により,次のようなPrimary Invariantsを生成するアルゴリズムが考えられる: Reynolds作用素によって Primary Invariants の候補 $\{p_1,\ldots,p_i\}$ を生成し, 新たに生成された $q$ が $q \notin \sqrt{\langle p_1,\ldots,p_i\rangle}$ なら $q := p_{i+1}$ として Primary Invariants の候補に付け加え, $q \in \sqrt{\langle p_1,\ldots,p_i\rangle}$ なら, $q$ を棄てて, 新たに Reynolds 作用素により不変式を生成する. このような生成手続きは生成された不変式 $p_1,\ldots,p_m$ が条件 (3) を満すとき終了する. しかし一般的には手続きが終了したとき, $m \geq n$ となっている. $m = n$ ならば, 得られた $p_1,\ldots,p_n$ が Primary Invariants であり, そうでない場合は $p_1,\ldots,p_m$ から適当に $n$ 個を選んで条件 (4) を調べる. 大抵の場合は $m$ 個の中から $p_1,\ldots,p_n$ の適当な組合わせを選べば, 条件 (4) が満されることが知られている.

上記で述べた Primary Invariants 生成のアルゴリズムにおいて必要な基本アルゴリズムは, ある多項式が与えられた生成元をもつイデアルの根基イデアルに属するかどうかを判定するアルゴリズムで, このアルゴリズムがグレブナー基底を用いて簡単に記述できることは良く知られている ([2],[3]).

$\mathbb{F}[p_1,\ldots,p_n]$ が Noether の正規化になる条件は (4) で与えられたが, これを調べるのは少し面倒である. そこで同値な条件であって, もう少し調べやすいものをイデアルの次元の概念を用いて記述する. 但し, ここで必要なのはイデアルの次元が零であるかどうかを判定することだけであるから, 一般的なイデアルの次元の定義は紙面の都合もあって省略する.

**命題 3.2** ([1]) $p_1,\ldots,p_m \in \mathbb{F}[x_1,\ldots,x_n]^\Gamma$ を次数が正の同次式とする. 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ が $\mathbb{F}[p_1,\ldots,p_m]$ 上, 整であるための必要十分条件は,

$$\dim(\langle p_1,\ldots,p_m\rangle) = 0.$$

であり, この条件を満たすとき $m \geq n$ が成り立つ. 特に $m = n$ のとき, 部分環 $\mathbb{F}[p_1,\ldots,p_n]$ が $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の Noether の正規化であるための必要十分条件は, $\dim(\langle p_1,\ldots,p_n\rangle) = 0$ である.

多項式環のイデアルの次元が零であるとは, そのイデアルの零点多様体が有限集合になることである. 一般に多項式環のイデアルの次元を計算することはそれほど容易ではないが, あるイデアルの次元が零であるかどうかを判定することはグレブナー基底を用いることにより容易に実行できる ([2],[3]).

我々は以上で述べた Primary Invariants を生成するアルゴリズムを実際の数式処理システムに実装することができる.

**アルゴリズム 3.3** Primary Invariants の生成
入力: 行列群 $\Gamma$ の生成元 $\pi_1,\ldots,\pi_k$
出力: 不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の同次な Primary Invariants
方法:
$\Gamma$ のすべての要素を生成する.
Reynolds 作用素を表わす行列 $R_\Gamma$ を生成する.
Hilbert 級数 $H_\Gamma(X)$ の有理表現を計算する.
$l := 2$
$m := 0$
**repeat**
Hilbert 級数の第 $l$ 項までの部分展開を計算する.
$d$ を部分展開の最高次の項の次数とする.

$c_d$ を部分展開の最高次の項の係数とする.
$m_1, \ldots, m_{\binom{n+d-1}{d}}$ を $\mathbb{F}[x_1, \ldots, x_n]_d$ の単項式とする.
**for** $j$ **from** 1 **to** $\binom{n+d-1}{d}$ **by** 1 **do**
  $R_\Gamma(m_j)$ を計算する.
  **if** $R_\Gamma(m_j) \neq 0$ **then**
    $R_\Gamma(m_j) \in \sqrt{\langle q_1, \ldots, q_m \rangle}$ かどうか調べる.
    **if** $R_\Gamma(m_j) \notin \sqrt{\langle q_1, \ldots, q_m \rangle}$ **then**
      $m := m + 1$
      $q_m := R_\Gamma(m_j)$
  **if** $|\{q_i | \deg(q_i) = d \text{ and } 1 \leq i \leq m\}| = c_d$ **then**
    **break**[of **for** loop]
$l := l + 1$
**until** $\dim(\langle q_1, \ldots, q_m \rangle) = 0$
**if** $m = n$ **then**
  **return** : $q_1, \ldots, q_n$
**else**
  $m$ 個の多項式 $q_1, \ldots, q_m$ の中から $n$ 個の多項式を選び, それによって生成される
  イデアルの次元が 0 であれば, 選んだ $n$ 個の多項式を出力する.

**注意** Hilbert 級数の係数は独立な同時不変式の最大個数を与え, 計算の高速化に役立っているが, アルゴリズム 3.3 ではこの上限を頼りにして一旦その上限の個数まで, Primary Invariants の候補 $Q$ になる同次不変式を Reynolds 作用素を用いて生成しようとする. その後 $Q$ で生成されるイデアルの次元を調べ, $Q$ が Primary Invariants かどうか判定している. このアルゴリズムを用いた場合, 多くの場合 Primary Invariants の候補を $n$ 個見つけた後も Primary Invariants の候補を探し続けることが起きてしまう. そこで, 新しい Primary Invariants の候補を見つけるたびに Primary Invariants の候補の数を確認し, それが $n$ 個以上になった時点ですぐに命題 3.2 の条件を調べるよう改善することができる. この改善により位数の大きな群では, 計算時間ををかなり節約できることがわかった.

## 3.2 Secondary Invariants の生成

この部分節では Secondary Invariants を生成するアルゴリズムについて述べる. 前の部分節ですでに Primary Invariant を求めるアルゴリズムについて述べたから, すでに Primary Invarints はすべて求まっていると仮定する. そのとき, Molien の定理より不変式環の広中分解に注目して次の結果が得られる ([13]) .

**定理 3.4** $\mathbb{F}[p_1, \ldots, p_n]$ を $\mathbb{F}[x_1, \ldots, x_n]^\Gamma$ の同次な Noether の正規化とする.

(1) $H_\Gamma(X)$ を Molien の定理で定まる Hilbert 級数とすれば

$$H_\Gamma(X) \cdot \prod_{i=1}^{n} (1 - X^{\deg(p_i)}) = b_1 X^{s_1} + b_2 X^{s_2} + \cdots + b_k X^{s_k} \tag{5}$$

は正の整数 $b_i$ を係数とする $X$ の多項式で, 係数 $b_i$ が, 次数 $s_i$ の同次な Secondary Invariants の数を与える.

(2) Secondary Invariants の総数は次の式で与えられる.

$$\frac{\deg(p_1)\cdots\deg(p_n)}{|\Gamma|} \tag{6}$$

この定理により, Secondary Invariants が存在する次数とその数を求めることができる. 従って, Secondary Invariants を求めるには, 与えられた次数 $d$ において, $d$ 次の Secondary Invariants を全て求めることが出来ればよい. そのとき不変式環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ において Primary Invariants $p_1,\ldots,p_n$ で生成されるイデアルを $\langle p_1,\ldots,p_n\rangle^\Gamma$ とおくと, 商多元環 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma/\langle p_1,\ldots,p_n\rangle^\Gamma$ は次元 $t$ が定理 3.4 の (6) で与えられる次数付のベクトル空間で, Secondary Invariants の属する剰余類 $s_i+\langle p_1,\ldots,p_n\rangle^\Gamma (i=1,\ldots,t)$ がそのベクトル空間の基底となる. 従って, 各次数 $d$ においてて $\mathbb{F}$ 上のベクトル空間

$$V_d=\{s+\langle p_1,\ldots,p_n\rangle^\Gamma \mid s\in\mathbb{F}[x_1,\ldots,x_n]_d^\Gamma\}$$

の基底を $d$ 次の同次不変式で見つけることができればよい. そのためには剰余類 $s+\langle p_1,\ldots,p_n\rangle^\Gamma$ が $\mathbb{F}$ 上 1 次独立となるものを探せばよい. そのような同次不変式の最大個数は定理 3.4 の (5) で計算される多項式の $X^d$ の係数で与えられる. ベクトル空間 $V_d$ の基底を見いだすには次の補題が重要な役割を果す ([1]).

**補題 3.5** $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の同次な Primary Invariants を $p_1,\ldots,p_n$, また $s'_1,\ldots,s'_{t_d}$ $(t_d\le\dim(V_d))$ を剰余類 $s'_j+\langle p_1,\ldots,p_n\rangle^\Gamma$ がベクトル空間 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma/\langle p_1,\ldots,p_n\rangle^\Gamma$ 内で $\mathbb{F}$ 上 1 次独立になるような $d$ 次の同次不変式とする. また $s$ を $d$ 次の同次不変式とする. そのとき, 次の主張は同値である.

(1) $\{s'_j+\langle p_1,\ldots,p_n\rangle^\Gamma \mid 1\le j\le t_d\}$ と $s+\langle p_1,\ldots,p_n\rangle^\Gamma$ は $\mathbb{F}[x_1,\ldots,x_n]^\Gamma/\langle p_1,\ldots,p_n\rangle^\Gamma$ で $\mathbb{F}$ 上 1 次独立である.

(2) $s\notin\langle s'_1,\ldots,s'_{t_d},p_1,\ldots,p_n\rangle^\Gamma\subset\mathbb{F}[x_1,\ldots,x_n]^\Gamma$

(3) $s\notin\langle s'_1,\ldots,s'_{t_d},p_1,\ldots,p_n\rangle\subset\mathbb{F}[x_1,\ldots,x_n]$

この補題の (1) と (2) の同値性は明らかである. この補題の本質は (3) にあり, 補題の (3) は同次不変式のベクトル空間 $\mathbb{F}[x_1,\ldots,x_n]^\Gamma/\langle p_1,\ldots,p_n\rangle^\Gamma$ における 1 次独立性の判定が, 多項式環 $\mathbb{F}[x_1,\ldots,x_n]$ におけるイデアルの所属問題 ([2],[3]) に帰着することを主張している. よって次のような Secondary Invariants の生成アルゴリズムが構成できる.

**アルゴリズム 3.6** Secondary Invariants の生成

入力: 同次な Primary Invariants $p_1,\ldots,p_n$, Reynolds 作用素を表わす行列 $R_\Gamma$, Hilbert 級数の有理表現 $H_\Gamma(X)$

出力: $\mathbb{F}[x_1,\ldots,x_n]^\Gamma$ の $\mathbb{F}[p_1,\ldots,p_n]$ 上の自由加群としての生成元である, 同次な Secondary Invariants

方法:

1変数多項式 $H_\Gamma(X)\cdot\prod_{i=1}^{n}(1-X^{\deg(p_i)})$ を計算し, その次数を $d'$ とする.
$0\le d\le d'$ について, $H_\Gamma(X)\cdot\prod_{i=1}^{n}(1-X^{\deg(p_i)})$ の $X^d$ の係数を $t_d\in\mathbb{N}_0$ とする.
$t:=0$
**for1** $d$ **from** 0 **to** $d'$ **by** 1 **do**
  **if1** $t_d\neq 0$ **then**
    $m_1,\ldots,m_{\binom{n+d-1}{d}}$ を $\mathbb{F}[x_1,\ldots,x_n]_d$ の単項式とする.
    **for2** $l$ **from** 1 **to** $\binom{n+d-1}{d}$ **by** 1 **do**
      $R_\Gamma(m_l)$ を計算する.
      **if2** $R_\Gamma(m_l)\notin\langle s_j|\ \deg(s_j)=d,\ 1\le j\le t\rangle+\langle p_1,\ldots,p_n\rangle$ **then**
        $t:=t+1$
        $s_t:=R_\Gamma(m_l)$
      **if3** $|\{s_j|\ \deg(s_j)=d,\ 1\le j\le t\}|=t_d$ **then**
        **break** [of **for2** loop]
**return** : $s_1,\ldots,s_t$

## 4 数式処理システム Asir での計算

本節では, Asir上で作成した不変式環の生成元を計算するプログラムの機能について具体例を挙げて説明する. このプログラムを使うにはまずコマンドラインで

```
asir
```

と入力すると

```
This is Risa/Asir, Version 20001017.
Copyright (C) FUJITSU LABORATORIES LIMITED.
1994-2000. All rights reserved.
[0]
```

と表示されて, Asirが起動する. 次に

```
load("gr")$
load("sp")$
load("finvar")$
```

と入力すると, グレブナー基底 (gr), 代数的数 (sp) のライブラリと今回作成した不変式のプログラム (finvar) が読み込まれ, プログラムを使う準備ができる.

まず簡単な例として, 平面上の $\frac{\pi}{2}$ (90°) の回転を表わす行列 $\pi_1$ で生成される4次の巡回群の Primary Invariants と Secondary Invariants を計算してみよう. 群 $\Gamma$ の生成元である $\frac{\pi}{2}$ の回転行列 $\pi_1=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ は,

```
Pai1 = newmat( 2, 2, [ [ 0, -1 ], [ 1, 0 ] ] );
```

と入力すると定義できる．ここで newmat の最初の２つの引数 2, 2 は入力される行列が２行２列の行列であることを示している．
次に，群 $\Gamma$ の生成元の集合 Gamma $= \{\pi_1\}$ を

```
Gamma = [ Pai1 ];
```

と入力して定義する．生成元が２つ以上ある場合は２番目の例を参照されたい．集合 Gamma の要素で生成される有限行列群 $\Gamma$ の不変式環の Primary Invariants と Secondary Invariants を求めるには

```
Invar = finvar( Gamma );
```

と入力すればよい．そのとき出力は

```
p1 = x1^2+x2^2
p2 = x1^4+x2^4
s1 = 1
s2 = -x2*x1^3+x2^3*x1
```

となり，Primary Invariants が $p_1 = x_1^2 + x_2^2$, $p_2 = x_1^4 + x_2^4$ , Secondary Invariants が $s_1 = 1$, $s_2 = x_1x_2^3 - x_1^3x_2$ であることが分かった．ここで，$p_1, p_2, s_1, s_2$ はリスト Invar に格納されている．次に，ある多項式が不変式環に属するかどうか調べ，属しているならば，広中分解により Primary Invarinats と Secondary Invariants で表わすことを考える．例として，多項式 $f = -4x_1^5x_2 + 3x_1^4 + 2x_1^2x_2^2 + 4x_1x_2^5 + 3x_2^4$ を考える．そのためには

```
mod_con ( Invar, -4*x1^5*x2+3*x1^4+2*x1^2*x2^2+4*x1*x2^5+3*x2^4 );
```

と入力する．そのとき出力は

```
true
4*p1*s2+p1^2+2*p2
```

となる．１番目の出力 true は $f$ が不変式であることを表わし，(不変式でない場合は false が出力される)．２番目の出力結果から $f$ が $p1, p2, s1, s2$ の組合わせで
$f = p_1^2 + 2p_2 + 4p_1s_2$ $(= s_1(p_1^2 + 2p_2) + s_2(4p_1) \in s_1\mathbb{F}[p_1, p_2] + s_2\mathbb{F}[p_1, p_2])$
と書けることが分かる．
次に，平方根や虚数を要素に含んだ行列 $\pi_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\pi_2 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix}$ で生成される有限行列群 $\Gamma$ の Primary Invariants と Secondary Invariants を計算してみる．
まず，$\sqrt{2}$ と $\sqrt{-1}$ を定義するために

```
Root2  = newalg( x^2 - 2 );
I      = newalg( x^2 + 1 );
```

と入力する．出力は

となり，$\sqrt{2}$ と $\sqrt{-1}$ が定義多項式 $x^2-2$, $x^2+1$ の根として定義される．これからはプログラムが (#0) と出力すれば $\sqrt{2}$, (#1) と出力すれば $\sqrt{-1}$ を表わすが，$\sqrt{2}$ と $\sqrt{-1}$ を代入するときには (#0) や (#1) は使えず，代わりに `Root2`，`I` を使う．すなわち，上記で定義された，平方根と虚数を要素に含んだ行列 $\pi_1$, $\pi_2$ を定義するには

```
Pai1 = newmat( 2, 2, [ [ 1, 1 ], [ 1, -1 ] ] );
Pai1 = Pai1 / Root2;
Pai2 = newmat( 2, 2, [ [ 1, 0 ], [ 0, I ] ] );
```

と入力すればよい．あとは前の計算例と同じように，生成元の集合 `Gamma` をリストで定義し，`finvar` で `Gamma` で生成される有限行列群の不変式を求めることができる．すなわち，

```
Gamma = [ Pai1, Pai2 ];
Invar = finvar( Gamma );
```

と入力すれば

```
p1 = x1^8+14*x2^4*x1^4+x2^8
p2 = 1025*x1^24+10626*x2^4*x1^20+735471*x2^8*x1^16+2704156*x2^12*x1^12
     +735471*x2^16*x1^8+10626*x2^20*x1^4+1025*x2^24
s1 = 1
```

と出力されて Primary Invariants と Secondary Invariants が計算できる．今の場合 Secondary Invariants は自明な元 1 しかなく，不変式環は Primary Invariants だけで生成される（$\Gamma$ は鏡映群となる）ことが分かる．この例に現れる有限行列群はある符号の weight enumerator の計算に必要な群 ([12]) で，群の位数は 192 である．

## 5 あとがき

今後の課題をいくつか挙げる:

- 今回作成したプログラムは，標数が 0 の場合にしか適用できないが，任意の標数の有限行列群の不変式環の生成元を計算するアルゴリズムはすでに知られているので ([1],[7])，そのアルゴリズムを Asir 上に実装すること．
- アルゴリズム 3.3 や 3.6 では，変数の数と次数を指定してひとまず，単項式をすべて生成してから，それらに対して Reynolds 作用素を作用させている．それに比べると，単項式を 1 つ生成するごとに Reynolds 作用素を作用させ，それらの不変式が Primary Invariants や Secondary Invariants になるかどうかを調べた方が余分な単項式の生成がない分，計算が速くなると予想される．しかし，今回の実装では有限行列群の不変式環の生成元を求めるアルゴリズムの理解と，とりあえず動くプログラムを作成することに重点を置いたので，細かな高速化は行っていない．

- 変数の数と次数を指定して単項式を生成するサブルーチン (gen_monomial) は，アルゴリズムを独自に考案して作成した．最初は単純でプログラムしやすいが速度が遅いアルゴリズムだったが，計算の高速化のために，樹形図を書く要領で変数の組み合わせを考え，単項式を生成するように改良した．これで計算速度は十分速くなったが，これよりも適切なアルゴリズムがあるかもしれない．

## 参 考 文 献


[1] Agnes, E. H. *Generating Invariant Rings of Finite Groups.* http://www.mat.dtu.dk/persons/Heydtmann_Agnes_Eileen/PS/th.ps,1996

[2] Becker, B and Weispfenning, V. *Gröbner Bases (2nd Ed).* Springer-Verlag,1998.

[3] Cox, D., J. Little and D. O'Shea *Ideals, Varieties, and Algorithms* 2nd Ed.Springer-Verlag, New York,1997.

[4] Decker,W. and Jong,T. *Gröbner Bases and Invariant Theory* in Buchberger,B and Winkler,F eds. *Gröbner Bases and Applications* London Math. Soc. Lect. Note Vol.251(1998),61–89, Cambridge Univ.Press

[5] Grove,L.C. and Benson,C.T *Finite Reflection Groups.* 2nd Ed. GTM 99,Springer-Verlag, New York,1996.

[6] Hochster, M., and Eagon, J.A. *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci.* Am. J. Math. **93**(1971), 1020-1058.

[7] Kemper, G. *Calculating Invariant Rings of Finite Groups over Arbitrary Fields.* J. Symbolic Computation **21**(1996), 351-366.

[8] Molien, T. *Über die Invarianten der linearen Substitutionsgruppen.* Sitzungsber. König. Preuss. Akad. Wiss.(1897), 1152-1156.

[9] 鍋島 勇，有限群の不変式環の生成-*Asir* による計算，同志社大学修士論文，2000,Feb.

[10] Noether,E. *Der Endlichkeitssatz der endlicher Gruppen* Math. Ann. **77**(1916),89-92.

[11] 齋藤 友克，竹島 卓，平野 照比古 著 **日本で生れた数式処理ソフト** (リサアジールガイドブック)，SEG 出版,1998.

[12] Sloane, N.J.A. *Error Correcting Codes and Invariant Theory: New Applications of a Nineteenth Century Technique.* Am. Math. Monthly **84**(1977), 82-107.

[13] Sturmfels, B. *Algorithms in Invariant Theory.* Springer-Verlag, Wien,1993.